RSAC 2025 Conference

Many Voices.
One Community.

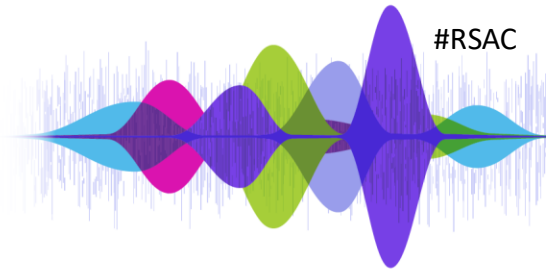
SESSION ID: LAB1-R01

Cyber Defense Matrix Workshop

Bryson Bort
Founder/CEO
SCYTHE

Pierre-David Oriol
Chief Product Officer
Inscora

Sounil Yu
Founder/CTO
Knostic



Disclaimer

Presentations are intended for educational purposes only and do not replace independent professional judgment. Statements of fact and opinions expressed are those of the presenters individually and, unless expressly stated to the contrary, are not the opinion or position of RSA Conference LLC or any other co-sponsors. RSA Conference LLC does not endorse or approve, and assumes no responsibility for, the content, accuracy or completeness of the information presented.

Attendees should note that sessions may be audio- or video-recorded and may be published in various media, including print, audio and video formats without further notice. The presentation template and any media capture are subject to copyright protection.

© 2025 RSA Conference LLC or its affiliates. The RSAC and RSAC CONFERENCE logos and other trademarks are proprietary. All rights reserved.

Our Disclaimers

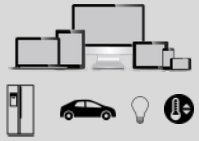
- Vendors shown are representative only
- No usage or endorsement should be construed because they are shown here
- Opinions are our own and do not represent those of our respective employers

What is missing?

Assets and functions help us create structure

Asset Classes

DEVICES



Workstations, servers, phones, tablets, storage, network devices, IoT infrastructure, etc.

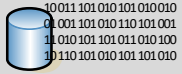
APPS

Software, interactions, and application flows on the devices

NETWORKS

Connections and traffic flowing among devices and apps

DATA



Information at rest, in transit, or in use by the resources above

USERS

The people using the resources listed above

Operational Functions

IDENTIFY

Inventorying assets and vulns, measuring attack surface, prioritizing, baselining normal, threat modeling, risk assessment

PROTECT

Preventing or limiting impact, patching, containing, isolating, hardening, managing access, vuln remediation

DETECT

Discovering events, triggering on anomalies, hunting for intrusions, security analytics

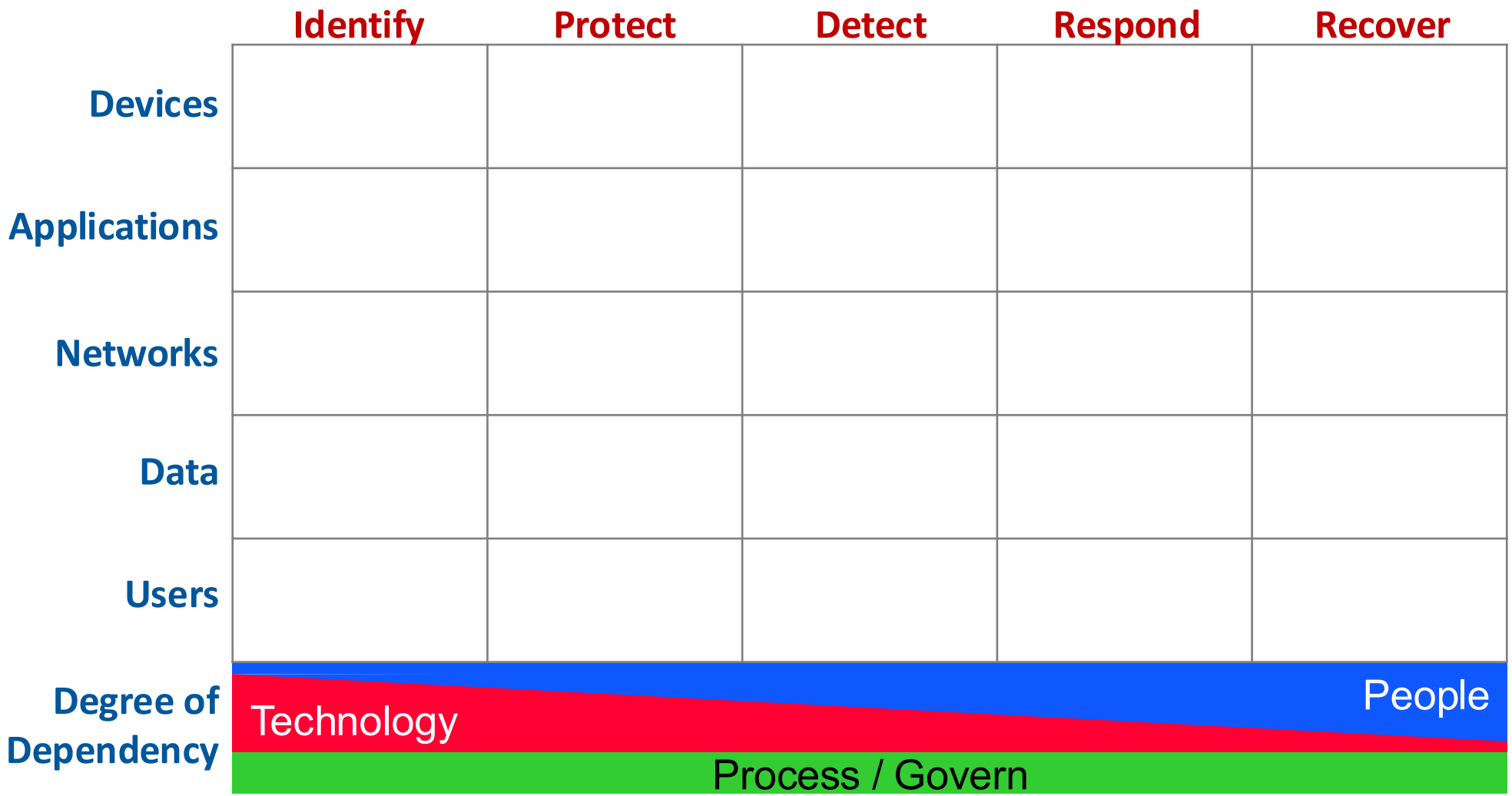
RESPOND

Acting on events, eradicating intrusion, assessing damage, forensic reconstruction

RECOVER

Returning to normal operations, restoring services, documenting lessons learned, resiliency

The Cyber Defense Matrix

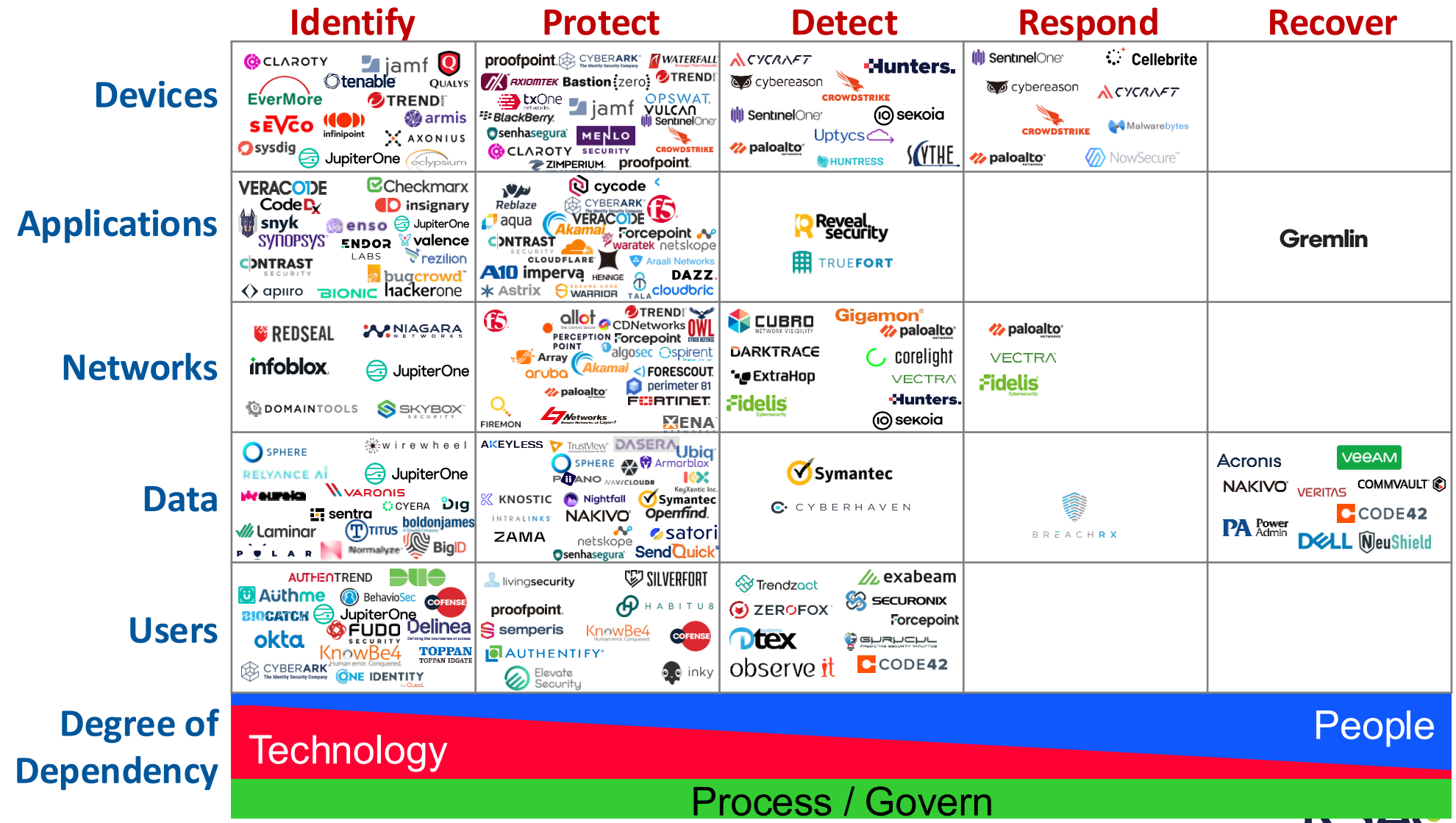


Aligning the Cyber Defense Matrix against the buzzwords…

… allow us to organize capabilities and see gaps…

	Identify	Protect	Detect	Respond	Recover
Devices	Asset Mgt, Vuln Scanning, Vuln Mgt, Certificate Mgt	AV, Anti-Malware, EPP, FIM, HIPS, Vuln Mitigation, Allowlisting	Endpoint Detection, UEBA, XDR	EP Response, EP Forensics, SOAR	
Applications	SAST, DAST, SW Asset Mgt, Fuzzers, Bug Bounty	RASP, WAF, ASOC, ZT App Access, API Security	Source Code Compromise, Logic Bomb Discovery, App IDS, XDR		
Networks	Netflow, Network Vuln Scanner	FW, IPS/IDS, Microseg, SEG, SWG, ZTNA	DDoS Detection, Net Traf Analysis, UEBA, XDR	DDoS Response, NW Forensics, SOAR	
Data	Data Discovery, Classification, Crypto Inventory, DSPM	Encryption, DRM, Tokenization, DLP, Backup, DBAM, DB Access Proxy	Deep Web, Data Behavior Analytics, FBI, Brian Krebs, XDR	DRM, Breach Response	Backup Recovery
Users	Phishing Sim, Background Chk, MFA, Human Risk Mgt	Sec Awareness & Training, Adaptive People Protection	Insider Threat, User Behavior Analytics, XDR, Human Det & Resp		
Degree of Dependency	People / Technology / Process / Govern				

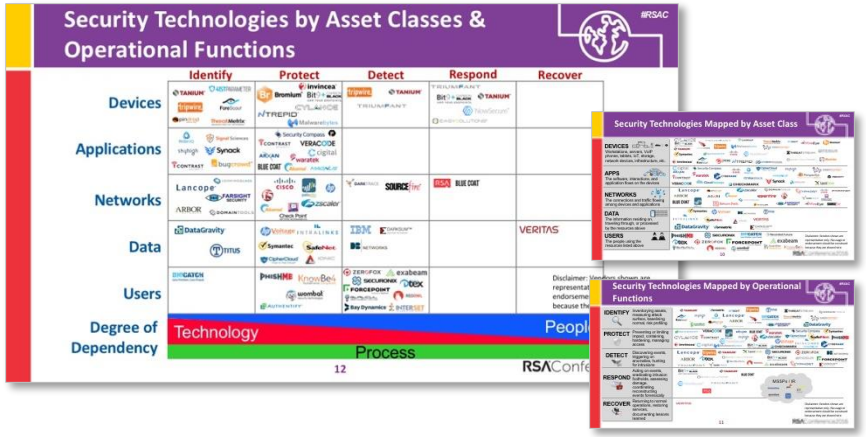
Mapping of Security Vendors

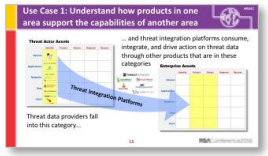


Use Cases of the Cyber Defense Matrix…

https://bit.ly/cyberdefensematrix

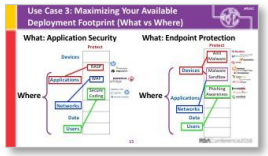
Primary Use Case: Vendor Mapping



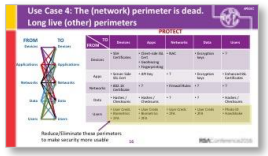


Differentiating Primary & Supporting Capabilities

Defining Security Design Patterns



Maximizing Deployment Footprint

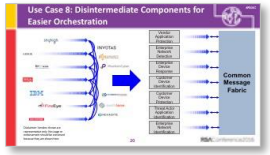


Understanding the New Perimeter

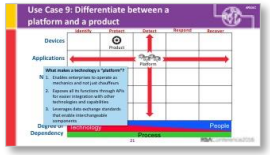
Calculating Defense-in-Breadth

Balancing Your Portfolio Budget

Planning for Obsolescence

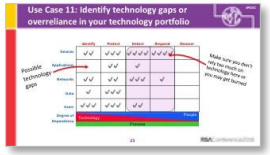


Disintermediating Security Components



Comparing Point Products vs Platforms

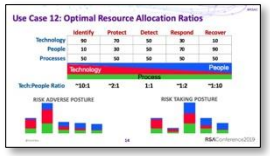
Finding Opportunities for Automation



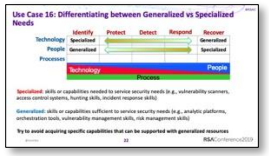
Identifying Gaps in People, Process, Tech

Other Use Cases of the Cyber Defense Matrix…

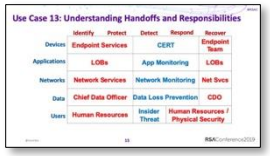
https://bit.ly/cyberdefensematrixreloaded



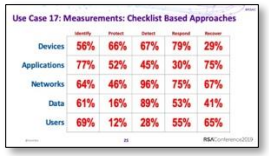
Optimizing Budgets and Resource Allocation



Aligning Generalized vs Specialized Needs



Mapping Organizational Handoffs

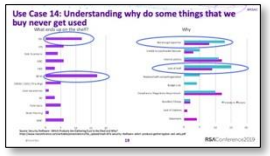


Measurements and Metrics

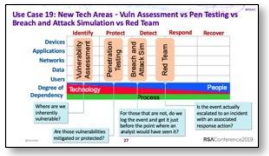
Aligning Roles and Responsibilities

Business Aligned Security Patterns

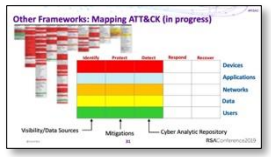
Mapping to the Kill Chain



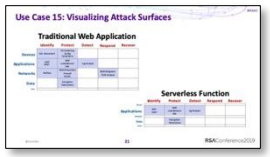
Understanding Why Products are Not Used



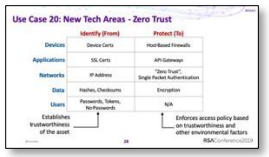
Vuln Scan vs PenTest vs BAS vs Red Team



Mapping to MITRE ATT&CK



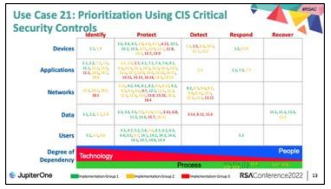
Visualizing Attack Surfaces



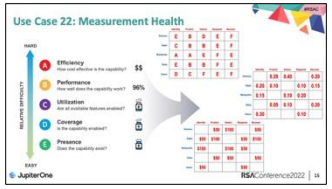
Mapping Zero Trust Capabilities

Other Use Cases of the Cyber Defense Matrix…

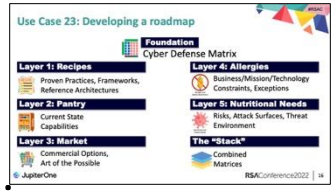
https://bit.ly/cyberdefensematrixrevolutions



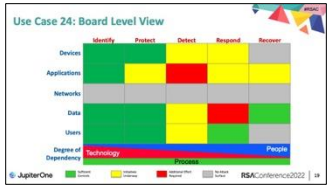
Mapping to CIS / Control prioritization



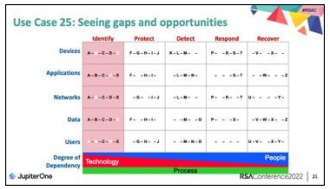
Measurement health



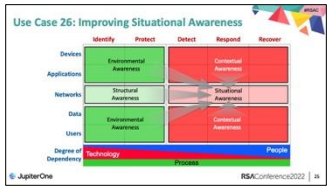
Building an infosec roadmap



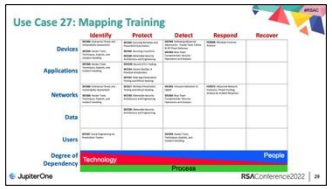
Creating board-level views



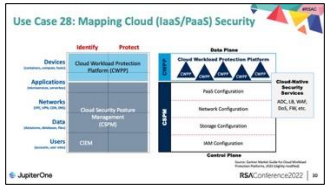
Finding gaps and startup opportunities



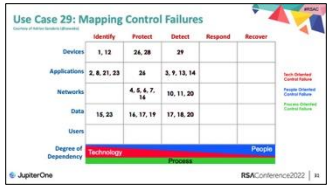
Improving Situational Awareness



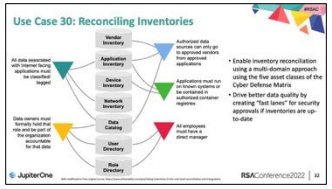
Mapping Training



Mapping Cloud Security Capabilities

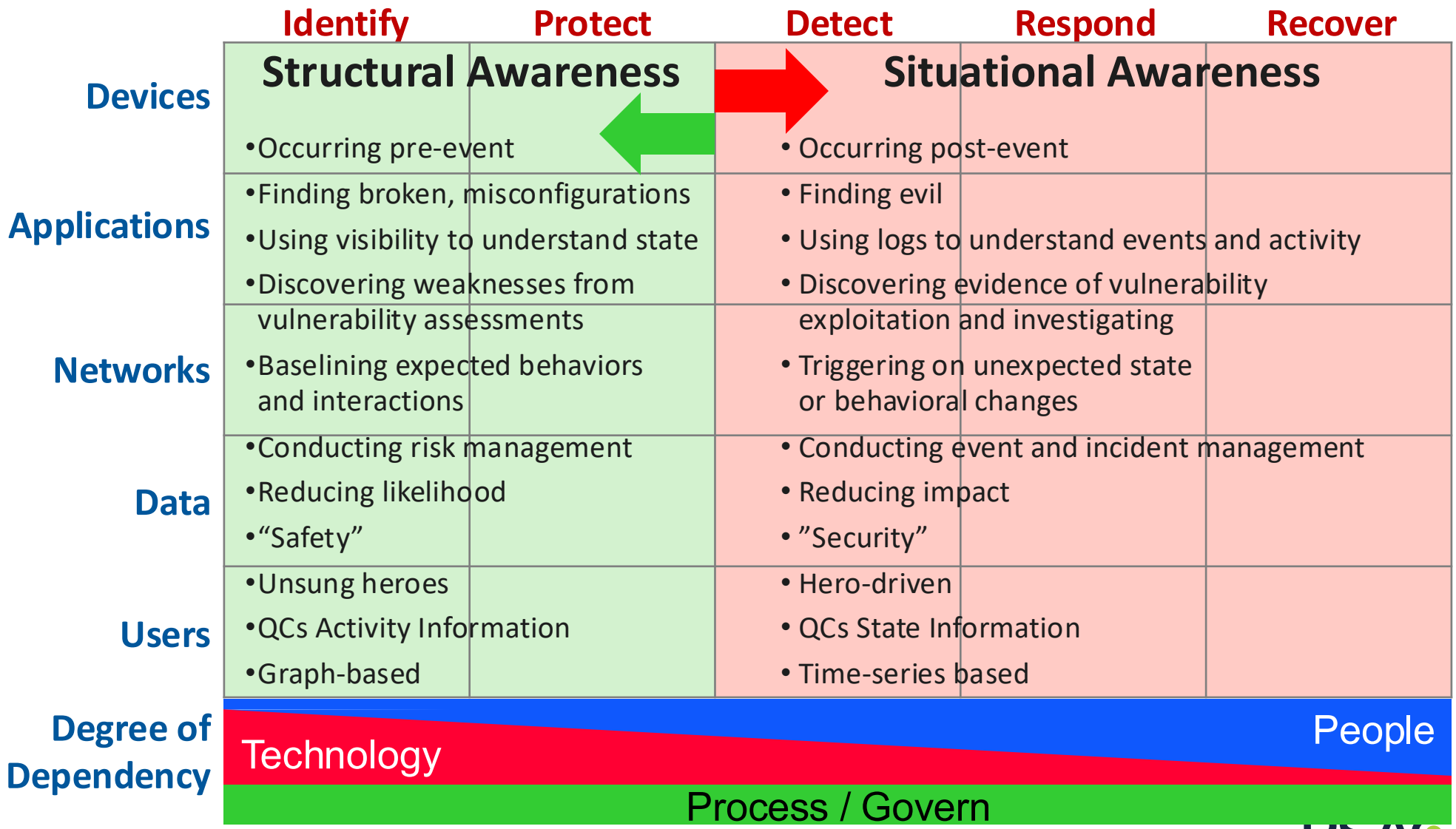


Mapping Control Failures



Reconciling Inventories

Terminology: Left & Right of "Boom"



RSAC 2025 Conference

Exercise 1: Mapping Product Categories

Sounil Yu
@sounilyu

Many Voices.
One Community.

Exercise 1: White House EO Edition

(https://bidenwhitehouse.archives.gov/briefing-room/presidential-actions/2025/01/16/executive-order-on-strengthening-and-promoting-innovation-in-the-nations-cybersecurity/)

	Identify	Protect	Detect	Respond	Recover	
Devices						Static Application Security Testing
Applications						Multi-Factor Authentication
Networks						
Data						Threat Hunting
Users						Zero Trust

Data Encryption

Network Segmentation

Endpoint Detection & Response

Software Bill of Materials

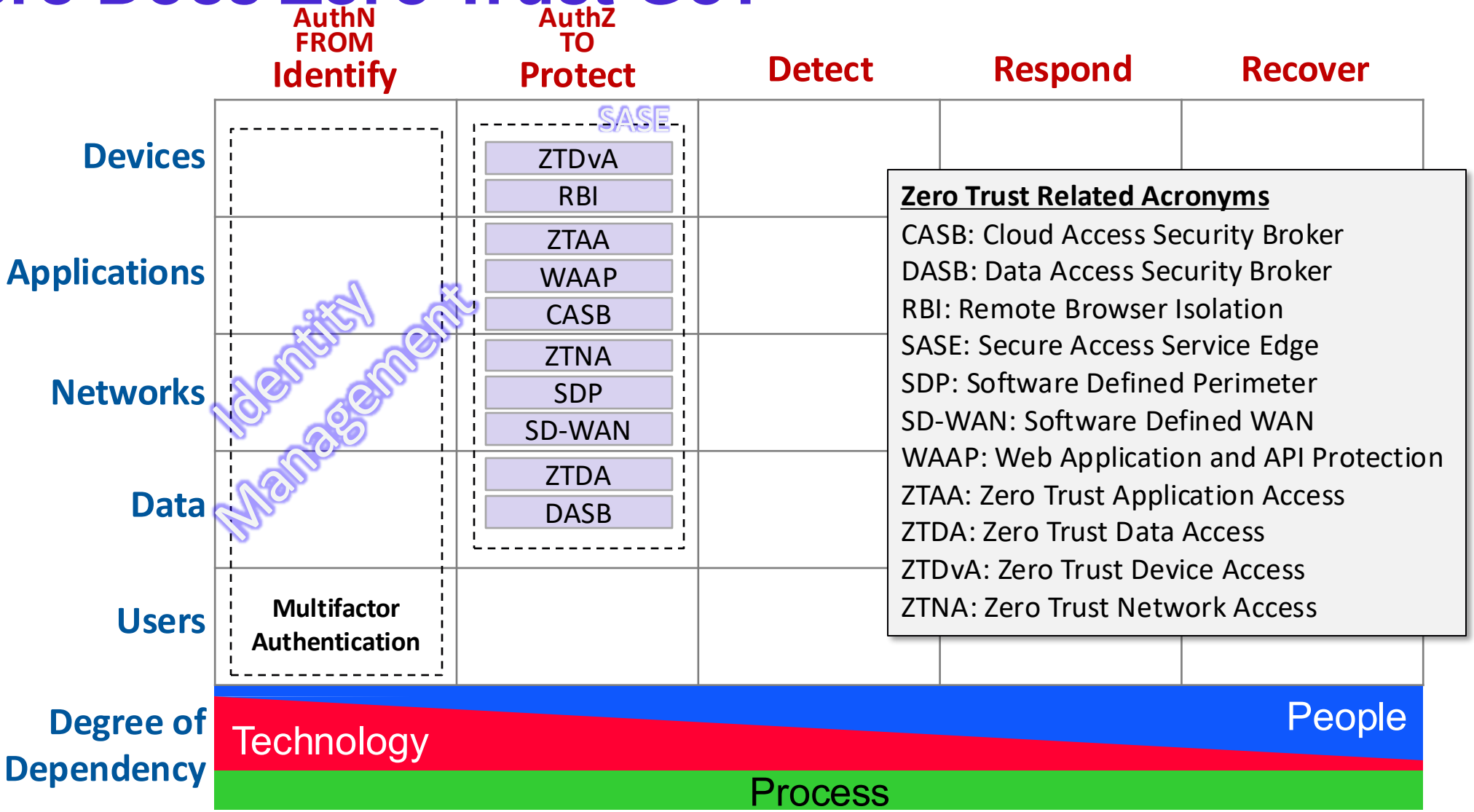
Degree of Dependency

Technology

People

Process / Govern

Where Does Zero Trust Go?



RSAC 2025 Conference

Exercise 2: Mapping Innovation Sandbox Vendors

Sounil Yu
@sounilyu

Many Voices.
One Community.

Exercise 2: RSA Innovation Sandbox Finalists

Aurascape

Calypso AI

CMD ZERO

EQTYLAB

KNOSTIC

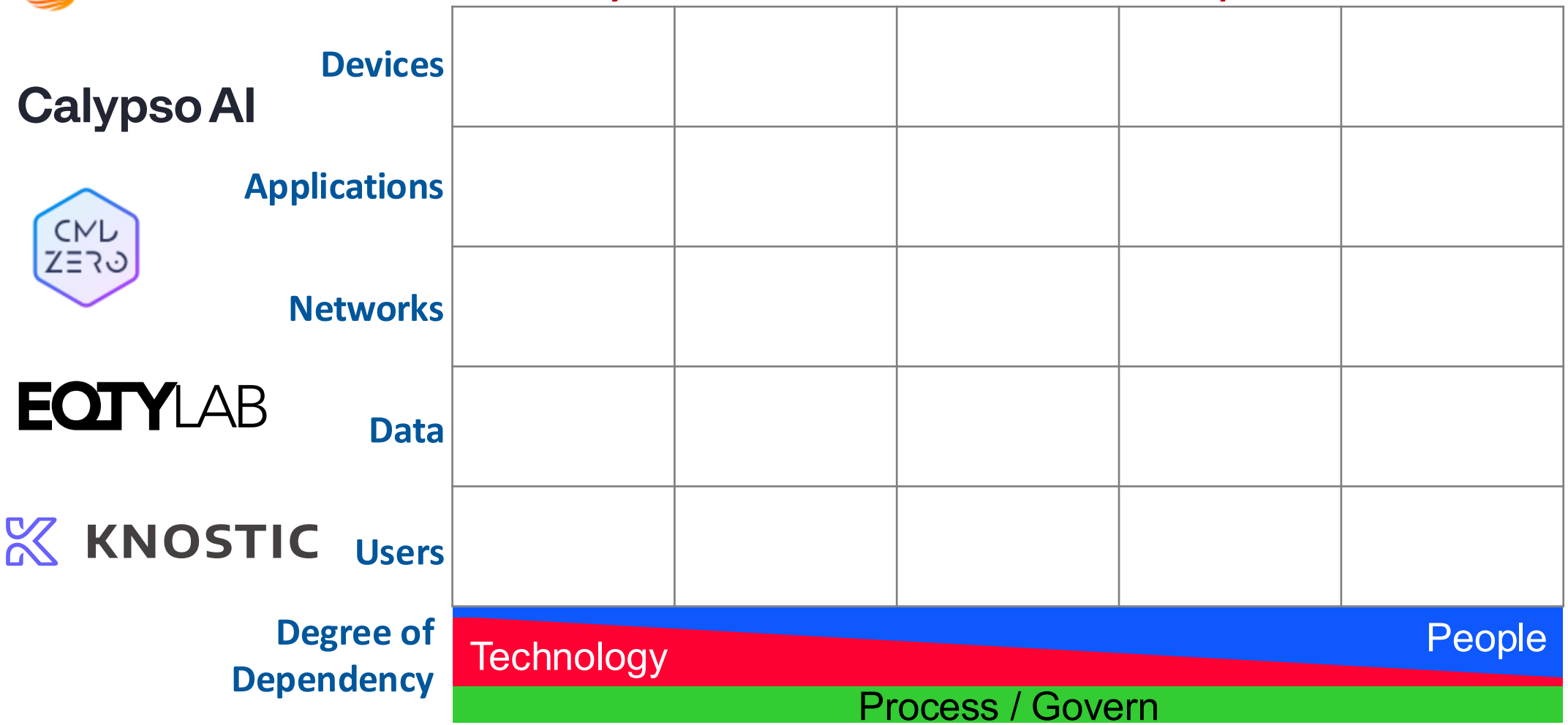
METALWARE

MIND

ProjectDiscovery

smallstep

twine



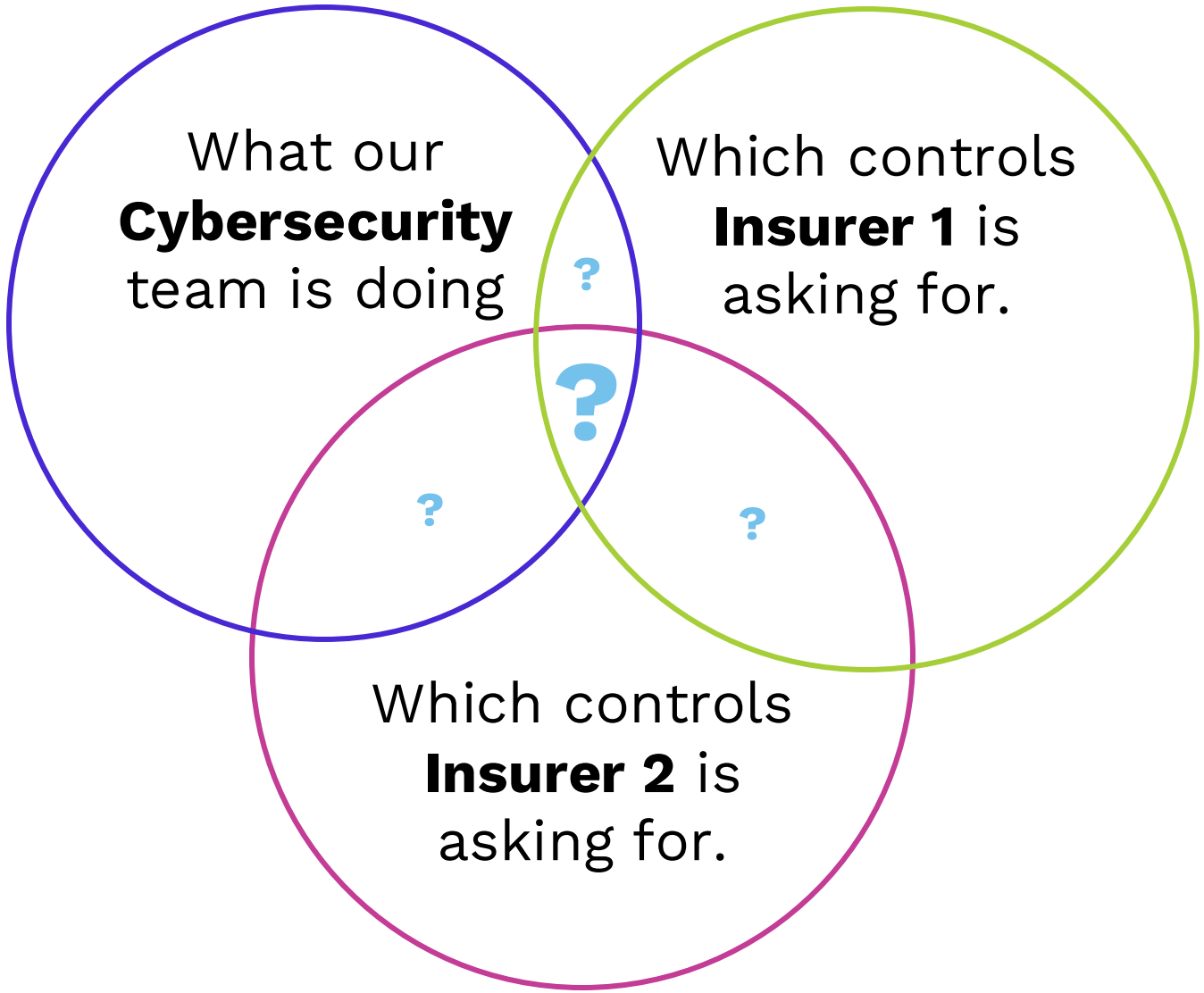
DISCLAIMER: NO VENDOR ENDORSEMENT IS IMPLIED. THESE WERE INDEPENDENTLY SELECTED.

RSAC 2025 Conference

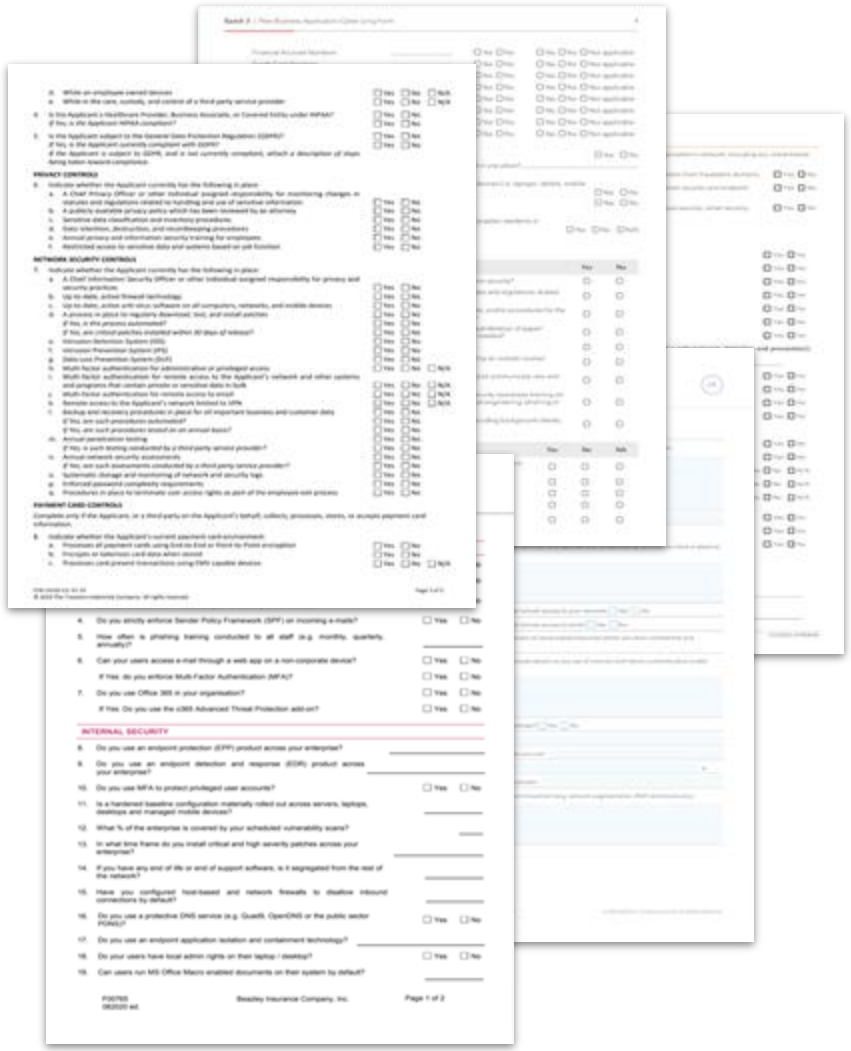
Exercise 3: Mapping Cyber Insurance Coverage Requirements

Pierre-David Oriol

Cyber Insurance Requirements - Intro



Cyber Insurance Requirements - Intro



Sample Questions from Cyber Insurance Application

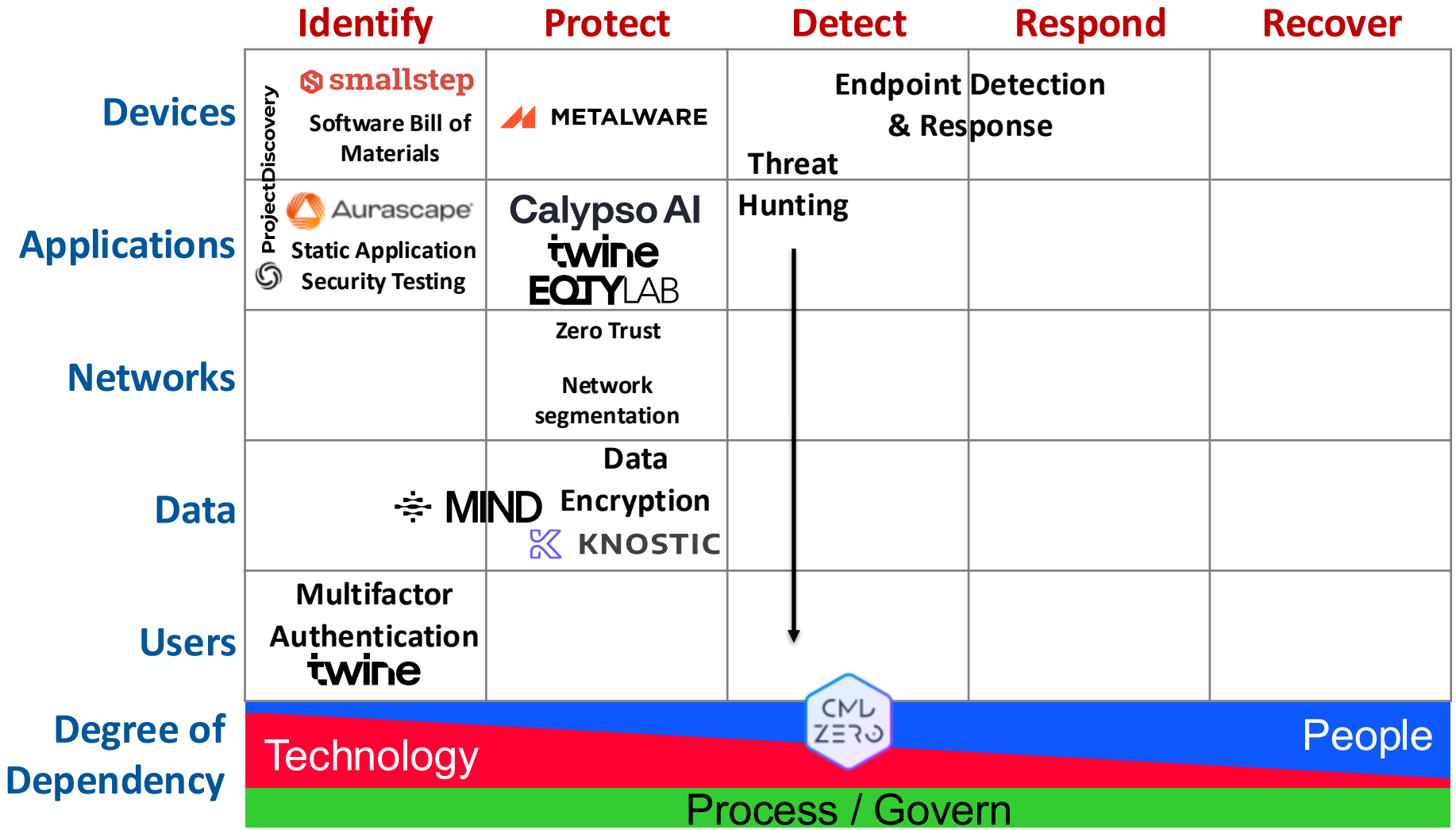
1. What % of your network is on-premise vs in the cloud?
2. Of cloud environments, what % of access is protected by MFA?
3. Do you leverage SSO for authentication to all cloud services?
4. How many servers / workstations do you supervise?
5. Do you possess a formal data classification policy?
6. Is RDP (or similar technology) used for remote access?
7. Do you make use of a FW to protect ALL your on-prem and/or cloud network?
8. Do you make use of SDNs?
9. Do you make use of an IDS or IPS?
10. What protective DNS service do you use to block known malicious websites?
11. What % of your endpoints have EDR?
12. Do you enforce application allowlisting/blocklisting via your EDR?
13. What % of your EDR & network events are centralized in an XDR alerting platform?
14. What % of your endpoints use application isolation and containment technology?
15. Can users access the network with BYOD?
16. If you possess a SIEM, what % of critical logs are fed into it?
17. Do you utilize a SOC?
18. What % of your global IT users have admin access to servers?
19. Is a Password Manager provided to all employees?
20. Which Vulnerability Mgt solution do you use (externally and internally)?

Exercise 3a: Choose the Best Fit Cyber Insurer

Navigate to: https://cdm.inscora.com

Exercise 3a: Choose the Best-Fit Cyber Insurer

Navigate to: https://cdm.inscora.com



DISCLAIMER: NO VENDOR ENDORSEMENT IS IMPLIED. THESE WERE INDEPENDENTLY SELECTED.

Exercise 3b: Choose the Best-Fit Cyber Insurer

Navigate to: https://cdm.inscora.com

Company profile: Cloud-Native SaaS Startup

Controls

- Cloud email access via Web + MFA & built-in security filtering
- Cloud-based firewall
- API-heavy - Scan & Real-time protection
- Uses K8S & Micro-segmented Network
- DNS-level DDoS protection / regularly tested
- Regular backups / tape-like cold storage
- EDR on workstations / DLP module enabled
- Mandatory security awareness training
- Centralized IAM management & reporting (PAM enforced via MFA)
- Data & Security Policies are managed via an outsourced vCISO service
- No SOC / SIEM or on-premises equipment

Insurance risk transfer objectives:

- Email Compromise / Social Engineering
- Ransomware
- Infostealers & Data Breaches

EXERCISE:

Using the Web app, you need to balance:

- Price point
- Effort (number of questions)
- Exclusions
- Carrier's requirements vs Current controls

RSAC 2025 Conference

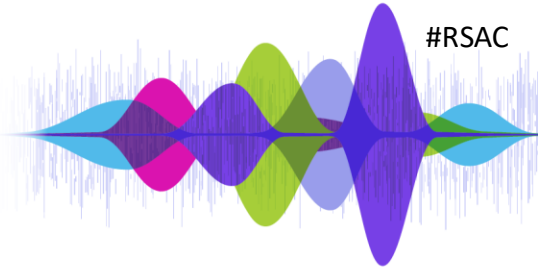
Exercise 4: Technology Rationalization

Bryson Bort

RSAC 2025 Conference

Wrap Up

Applying What You've Learned



- Map your security organization to the Cyber Defense Matrix
- Try out the use cases described here, in the previous briefings, and in the Cyber Defense Matrix book
- Develop a new use case for the Cyber Defense Matrix
- Share the new use case with the community!

RSAC™ | 2025 Conference

Many Voices.
One Community.